(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 March 2003 (27.03.2003)

PCT

(10) International Publication Number
WO 03/025868 A1

(51) International Patent Classification[7]: G07F 19/00, G06F 157/00

(21) International Application Number: PCT/AU02/01269

(22) International Filing Date:
17 September 2002 (17.09.2002)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PR 7726 17 September 2001 (17.09.2001) AU
PS 0920 7 March 2002 (07.03.2002) AU

(71) Applicant *(for all designated States except US)*: **INTERLINE NETWORKS PTY LTD** [AU/AU]; Suite 301, Level 3, 121 Walker Street, NORTH SYDNEY, New South Wales 2060 (AU).

(72) Inventor; and

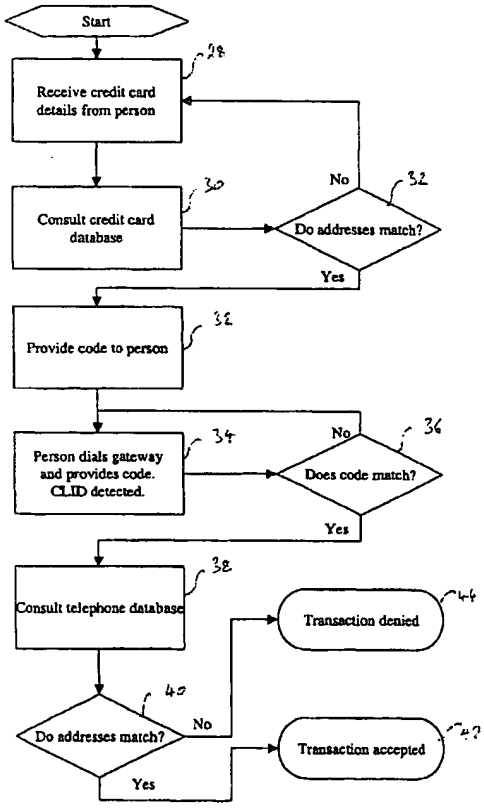
(75) Inventor/Applicant *(for US only)*: **PANDEYA, Hans** [AU/AU]; c/o Interline Networks Pty Ltd, Suite 301, Level 3, 121 Walker Street, NORTH SYDNEY, New South Wales 2060 (AU).

(74) Agent: **GRIFFITH HACK**; GPO Box 4164, Sydney, New South Wales 2001 (AU).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

[Continued on next page]

(54) Title: A METHOD AND SYSTEM FOR REDUCING THE RISK OF CREDIT CARD FRAUD



(57) Abstract: A method of reducing credit card fraud including the steps of receiving credit card information including a credit card number from a person (14) wishing to make a transaction (28); receiving a telephone call and verifying that the caller is the person (14) who supplied the credit card information (32); receiving authentication information by way of the telephone call (34); and using the authentication information to retrieve a previously authenticated address for the person (38). By this method, a previously authenticated address (38) is obtained for the person (14) making the transaction. This acts as a safeguard against fraudulent transactions because should it transpire that the credit card number provided by the person (14) was not their credit card number, they can subsequently be located using the previously authenticated address (38).

WO 03/025868 A1

(84) **Designated States** *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

A METHOD AND SYSTEM FOR REDUCING THE RISK OF CREDIT CARD FRAUD

Technical Field

This invention relates to a method and system for reducing the risk of credit card fraud.

Background to the Invention

At the time a person opens a credit card account, they are usually required to prove their identity by providing evidence in the form of a passport, drivers licence or birth certificate or the like. They are also required to authenticate an address to be associated with the account and usually must prove that they are connected with the address by providing examples of correspondence that they have received at that address such as bank statements or utility bills. Once the creditworthiness of the person at the given address has been checked and the person has been approved, the persons connection with the address is verified by mailing the credit card to this address. Thereafter, this authenticated address is used as the mailing address for mail order products that are purchased using the credit card. This system ensures that, even if the credit card is used fraudulently, any goods ordered will be despatched to the true account holder.

Some services may be purchased which do not need to be provided at the address of a credit card holder. For instance, certain internet based vendors offer services in return for payment. The services may be used at a website and do not involve any delivery to a physical postal address. Thus, the above mechanism does not assist in preventing fraudulent use. For instance, a user may wish to purchase credit on an account set up with an internet vendor for the purpose of sending SMS messages from a

website, or gambling at an online casino. These vendors may accept payment by credit card for these services. A fraudulent user could pay for these services by providing details of a live credit card account of which they are not the account holder.

There is a need for an arrangement which would ameliorate the above problem.

Summary of the Invention

In a first aspect the present invention provides a method of reducing credit card fraud including the steps of receiving credit card information including a credit card number from a person wishing to make a transaction; receiving a telephone call and verifying that the caller is the person who supplied the credit card information; receiving authentication information by way of the telephone call; and
using the authentication information to retrieve a previously authenticated address for the person.

By the above method, a previously authenticated address is obtained for the person making the transaction. This acts as a safeguard against fraudulent transaction because should it transpire that the credit card number provided by the person was fraudulent such as for instance by not being their credit card, they can subsequently be located using the previously authenticated address.

A previously authenticated address is an address that has been previously authenticated as being connected with the person. The address may be authenticated such as by the person proving that they live at the address or otherwise have access to the address by providing items of mail received at that address such as utility bills, by providing evidence in the form of official correspondence

received at that address or by providing evidence that they have received correspondence at that address sent by the organisation wishing to authenticate the address.

The step of verifying that the caller is the person who supplied the credit information may include the step of receiving the credit card information from the person making the telephone call. If the person provides the credit card information during the telephone call then it can be deduced that the person providing the credit card information is the same person that is making the telephone call.

The step of verifying that the caller is the person who supplied the credit card information may include the step of providing the person who supplied the credit card information with a security code; receiving a security code from the caller and matching the received security code with a supplied security code. The matching of security codes provides a simple way of correlating a person making a telephone call with the details they previously provided. Further, it ensures that they had access to the provided security code.

The step of receiving authentication information by way of the telephone call may include the step of receiving caller line identification information transmitted with the telephone call.

The step of receiving authentication information by way of the telephone call may include the step of receiving a user name and password from the caller.

The method may further include the step of verifying that the previously authenticated address is substantially the same as an address associated with the credit card number; and accepting the transaction only if the verification is successful.

The method may further include the step of verifying that the previously authenticated address is substantially the same as an address associated with the telephone account that was used to make the telephone call; and accepting the transaction only if the verification is successful.

An address is substantially the same as another address if it identifies the same physical location. For instance, if two addresses differ only in respect that one contains the term "street" and the other the abbreviation "st" then they identify the same physical location.

If it can be verified that the person has previously authenticated an address that is the same as an address associated with either a telephone account to which the person has access or that is the same as an address associated with the credit card then this indicates that the person is in some way connected with the address. This reduces the risk of accepting a transaction from an unauthorised person.

Optionally, the step of verifying that the previously authenticated address is substantially the same as an address associated with the telephone account further includes the step of providing the previously authenticated address to a telephone account database controller and receiving an indication of whether a telephone address stored in the telephone database is substantially the same as the previously authenticated address. Some telephone companies do not give out addresses associated with telephone numbers upon request. They may, however, advise whether a supplied address is the same, or substantially the same, as an address stored in a telephone database which is under their control.

Optionally, the credit card information includes an

address associated with the credit card number.

Optionally, the step of receiving the credit card information is done by way of the person interacting with a computer user interface.

Optionally, the computer user interface is provided at an internet website.

In a second aspect the present invention provides a system for reducing credit card fraud including means for receiving credit card information including a credit card number from a person wishing to make a transaction; means for receiving a telephone call and verifying that the caller is the person who supplied the credit card information; means for receiving authentication information by way of the telephone call; and means for using the authentication information to retrieve a previously authenticated address for the person.

The means for verifying that the caller is the person who supplied the credit card information may include means for providing the person who supplied the credit card information with a security code; means for receiving a security code from the caller and means for matching the received security code with a supplied security code.

The means for receiving authentication information by way of the telephone call may include means for receiving caller line identification information transmitted with the telephone call.

The means for receiving authentication information by way of the telephone call may include means for receiving a user name and password from the caller.

The system may further include means for verifying that the previously authenticated address is substantially the same as an address associated with the credit card number; and means for accepting the transaction only if

the verification is successful.

The system may further include means for verifying that the previously authenticated address is substantially the same as an address associated with the telephone account that was used to make the telephone call; and means for accepting the transaction only if the verification is successful.

Optionally, the means for verifying that the previously authenticated address is substantially the same as an address associated with the telephone account further includes means for providing the previously authenticated address to a telephone account database controller and means for receiving an indication of whether a telephone address stored in the telephone database is substantially the same as the previously authenticated address.

The credit card information may include an address associated with the credit card number.

The means for receiving the credit card information may include a computer user interface.

The computer user interface may be provided at an internet website.

In a third aspect the present invention provides a computer program providing instructions for controlling a computing system to carry out a method according to the first aspect of the invention.

In a fourth aspect the present invention provides a computer readable medium providing a computer program according to the third aspect of the invention.

Brief Description of the Drawings

An embodiment of the present invention will now be described, by way of example only, with reference to the

accompanying drawings, in which:

Figure 1 is a schematic view of an embodiment of a system for reducing the risk of credit card fraud according to the present invention; and

Figure 2 is a flow chart illustrating the steps of an embodiment of a method of reducing the risk of credit card fraud according to the present invention.

Detailed Description of the Preferred Embodiment

Referring to Figure 1, a system 10 is shown including receiving means, in this example embodied in server 12. The server can receive credit card details from a person 14 wishing to make a transaction over the internet 16. The person 14 can view an interface included in an internet website displayed on user interface 18. The software code required to display the interface is stored on server 12. This code may alternatively be stored on another computer connected to the internet.

The person 14 has a telephone 24 which may be used to dial in to telephone gateway 26. This telephone may be either of a traditional land line telephone or a mobile telephone.

The server 12 has access to a database of credit card information 20 and a database of telephone information 22. The credit card database would typically be operated and maintained by the credit card company responsible for the particular card. Indeed, a variety of credit card databases operated by various credit card companies are preferably accessible by the system. Similarly, the database of telephone information would typically be operated and maintained by a telephone company.

Both the credit card database and the database of telephone information include details of previously

authenticated addresses associated with the respective credit card and telephone accounts.

The system of the invention would typically be operated by a checking entity that performs security checks on behalf of a merchant. Operation of the system will now be described with reference to the method illustrated by Figure 2. Initially, at step 28 the person 14 that desires to make a transaction provides their credit card information, including the address of the credit card, using the website interface. These details are received by receiving means embodied in server 12.

At step 30, retrieving means embodied in server 12 retrieves a previously authenticated credit card address associated with the credit card number from credit card database 20.

At step 32, verifying means embodied in server 12 verifies that the address provided in the credit card information is substantially the same as the previously authenticated address obtained from credit card database 20. This is done using a software routine running on server 12 which applies an algorithm to compare the two addresses that allows for minor variations in address format. For example, the term "street" is taken to match the common abbreviation "st". If the addresses do not match then the method returns to step 28. If they do match the method proceeds to step 32.

At step 32, providing means embodied in server 12 provides a security code to person 14 by causing the security code to be displayed on their user interface. Further, the person is instructed to dial a telephone number, also provided by display on the user interface.

At step 34, the person uses telephone 24 to dial into gateway 26. Gateway 26 identifies the originating

telephone number of the telephone call from the caller line identification information that is transmitted at the time the telephone call is placed. The person is instructed by voice prompts to provide the security code with which they were provided at step 32. This may be done by manual entry using the telephone keypad, or by voice recognition techniques. Receiving means embodied in server 12 receives the security code that the person 14 provides.

At step 36, matching means embodied in server 12 matches the security code provided by person 14 with a security code previously provided by the system. If the security code does not match the method returns to step 34. If the security code does match the method proceeds to step 38.

At step 38, verifying means embodied in server 12 verifies that a telephone address stored in telephone database 22 and associated with the originating telephone number is substantially the same as the credit card address. This may be done by obtaining the telephone address from the database and comparing the addresses in the same manner as the previously described comparison of credit card addresses. Some telephone companies will not give out a telephone address when provided with only a telephone number. They may, however, confirm whether a provided address is substantially the same as an address stored in their telephone database and associated with a particular telephone number. If the addresses are substantially the same the method proceeds to step 42 and the transaction is accepted. If the addresses are not substantially the same the method proceeds to step 44 and the transaction is denied.

In the case of a person dialling into gateway 26 using a mobile telephone, additional verification may be made to allow for the fact that it is relatively easy to set up a mobile telephone account with a fraudulent address such as in the case of a pre-paid mobile telephone account where the mobile phone operator does not require the person to authenticate their address at the time of setting up their account. For this reason, the system may require that a person who wishes to call in using a mobile telephone previously authenticates an address associated with that mobile telephone number. This can be done by providing copies of correspondence received at that address. The authenticated address is then retrieved and used as the telephone address for the purposes of assessing the transaction.

The present invention has particular application for authenticating purchases for services which are not rendered at the address associated with the credit card. However, there is no reason why it could not be applied to authenticating purchases for physical goods being delivered to an address, for added security.

The method and system of the invention can be used to authenticate purchases of:

- Applying credit to an account at an internet based service which allows users to transfer money by email
- Airline tickets being picked up at check-in
- Paying for parking

It can be seen that the above described method and system provide an improved way of reducing the risk of credit card fraud by verifying that a person is associated with an address associated with a credit card.

It will be appreciated that, although described with reference to a transaction occurring over the internet, the invention is not limited to that use and can be used for transactions made over the telephone.

The system is not limited to databases including previously authenticated addresses relating to credit card or telephone accounts. Any database including previously authenticated address information can be used where that database includes details of the person. In one embodiment the system is operated for employees of a company and the company database of employee information is used to provide previously authenticated addresses. The validation information that is obtained from the person is their user name and password for accessing the company employee database.

It will be appreciated that, although the specific embodiment of the method described above is carried out using computer systems, in other embodiments some human involvement may be used to perform the invention such as call centre operators.

It will be appreciated that the above described embodiment is carried out using a combination of computer hardware and software. Any suitable computing system can be used such as networked computers or computers connected by dedicated connections.

Any reference to prior art contained herein is not to be taken as an admission that the information is common general knowledge, unless otherwise indicated.

Finally, it is to be appreciated that various alterations or additions may be made to the parts previously described without departing from the spirit or ambit of the present invention.

CLAIMS:

1. A method of reducing credit card fraud including the steps of:

receiving credit card information including a credit card number from a person wishing to make a transaction;

receiving a telephone call and verifying that the caller is the person who supplied the credit card information;

receiving authentication information by way of the telephone call; and

using the authentication information to retrieve a previously authenticated address for the person.

2. A method according to claim 1 wherein the step of verifying that the caller is the person who supplied the credit information further includes the step of receiving the credit card information from the person making the telephone call.

3. A method according to claim 1 wherein the step of verifying that the caller is the person who supplied the credit card information further includes the step of providing the person who supplied the credit card information with a security code; receiving a security code from the caller and matching the received security code with a supplied security code.

4. A method according to any preceding claim wherein the step of receiving authentication information by way of the telephone call further includes the step of receiving caller line identification information transmitted with the telephone call.

5. A method according to any preceding claim wherein the step of receiving authentication information by way

of the telephone call further includes the step of receiving a user name and password from the caller.

6. A method according to any preceding claim wherein further including the steps of verifying that the previously authenticated address is substantially the same as an address associated with the credit card number; and accepting the transaction only if the verification is successful.

7. A method according to any one of claims 1 to 5 further including the steps of verifying that the previously authenticated address is substantially the same as an address associated with the telephone account that was used to make the telephone call; and accepting the transaction only if the verification is successful.

8. A method according to claim 7 wherein the step of verifying that the previously authenticated address is substantially the same as an address associated with the telephone account further includes the steps of providing the previously authenticated address to a telephone account database controller and receiving an indication of whether a telephone address stored in the telephone database is substantially the same as the previously authenticated address.

9. A method according to any preceding claim wherein the credit card information includes an address associated with the credit card number.

10. A method according to any preceding claim wherein the step of receiving the credit card information is done by way of the person interacting with a computer user interface.

11. A method according to claim 10 wherein the computer user interface is provided at an internet website.

12. A system for reducing credit card fraud including:
means for receiving credit card information including a credit card number from a person wishing to make a transaction;
means for receiving a telephone call and verifying that the caller is the person who supplied the credit card information;
means for receiving authentication information by way of the telephone call; and
means for using the authentication information to retrieve a previously authenticated address for the person.

13. A system according to claim 12 wherein the means for verifying that the caller is the person who supplied the credit card information includes means for providing the person who supplied the credit card information with a security code; means for receiving a security code from the caller and means for matching the received security code with a supplied security code.

14. A system according to either claim 12 or claim 13 wherein the means for receiving authentication information by way of the telephone call includes means for receiving caller line identification information transmitted with the telephone call.

15. A system according to any one of claims 12 to 14 wherein the means for receiving authentication information by way of the telephone call includes means for receiving a user name and password from the caller.

16. A system according to any one of claims 12 to 15 further including means for verifying that the previously authenticated address is substantially the

same as an address associated with the credit card number; and means for accepting the transaction only if the verification is successful.

17. A system according to any one of claims 12 to 15 further including means for verifying that the previously authenticated address is substantially the same as an address associated with the telephone account that was used to make the telephone call; and means for accepting the transaction only if the verification is successful.

18. A system according to claim 17 wherein the means for verifying that the previously authenticated address is substantially the same as an address associated with the telephone account further includes means for providing the previously authenticated address to a telephone account database controller and means for receiving an indication of whether a telephone address stored in the telephone database is substantially the same as the previously authenticated address.

19. A system according to any one of claims 12 to 18 wherein the credit card information includes an address associated with the credit card number.

20. A system according to any one of claims 12 to wherein the means for receiving the credit card information includes a computer user interface.

21. A system according to claim 20 wherein the computer user interface is provided at an internet website.

22. A computer program providing instructions for controlling a computing system to carry out a method according to any one of claims 1 to 11.

23. A computer readable medium providing a computer program according to claim 22.

Dated this 17th day of September 2002

INTERLINE NETWORKS PTY LTD

By their Patent Attorneys

GRIFFITH HACK

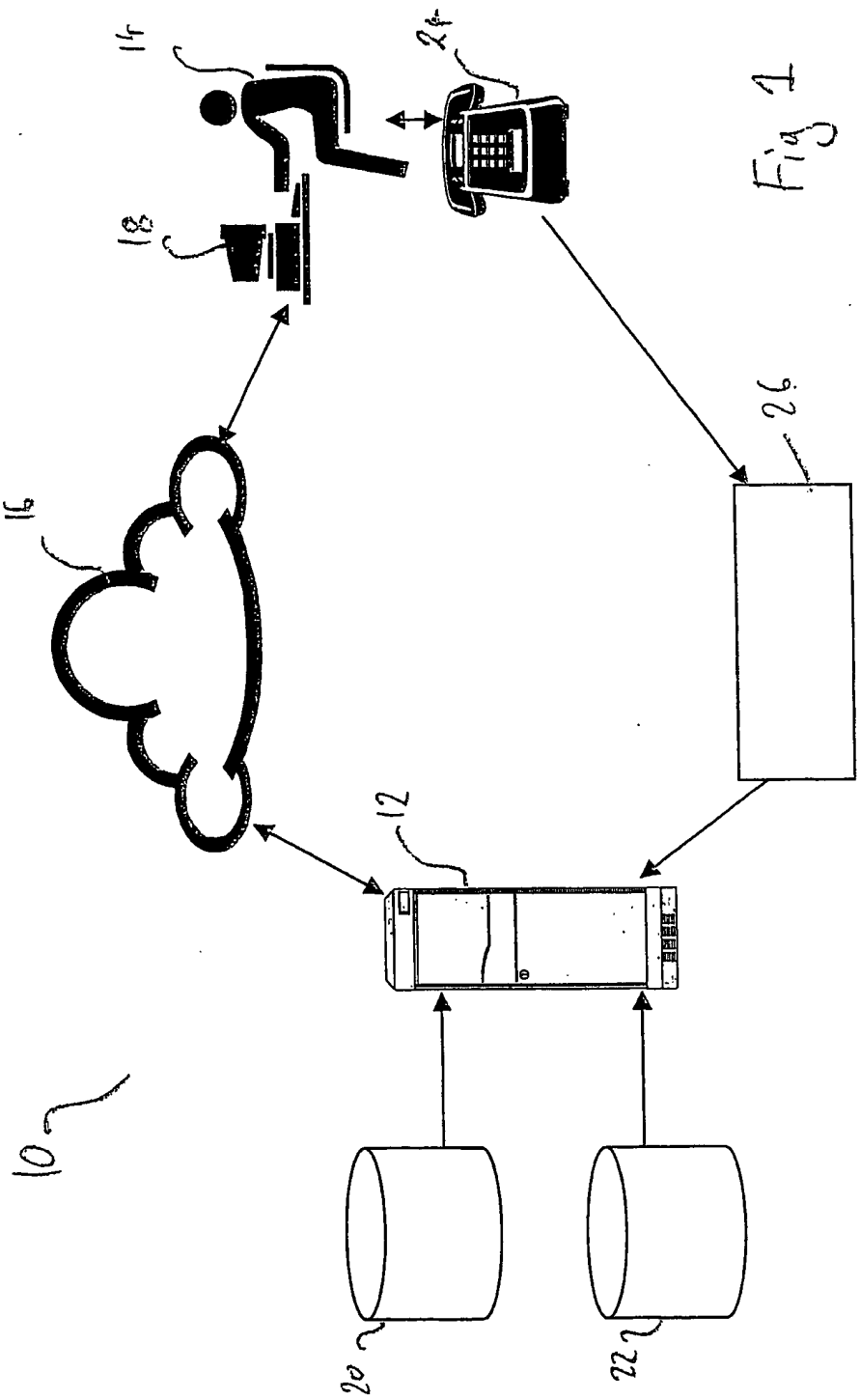
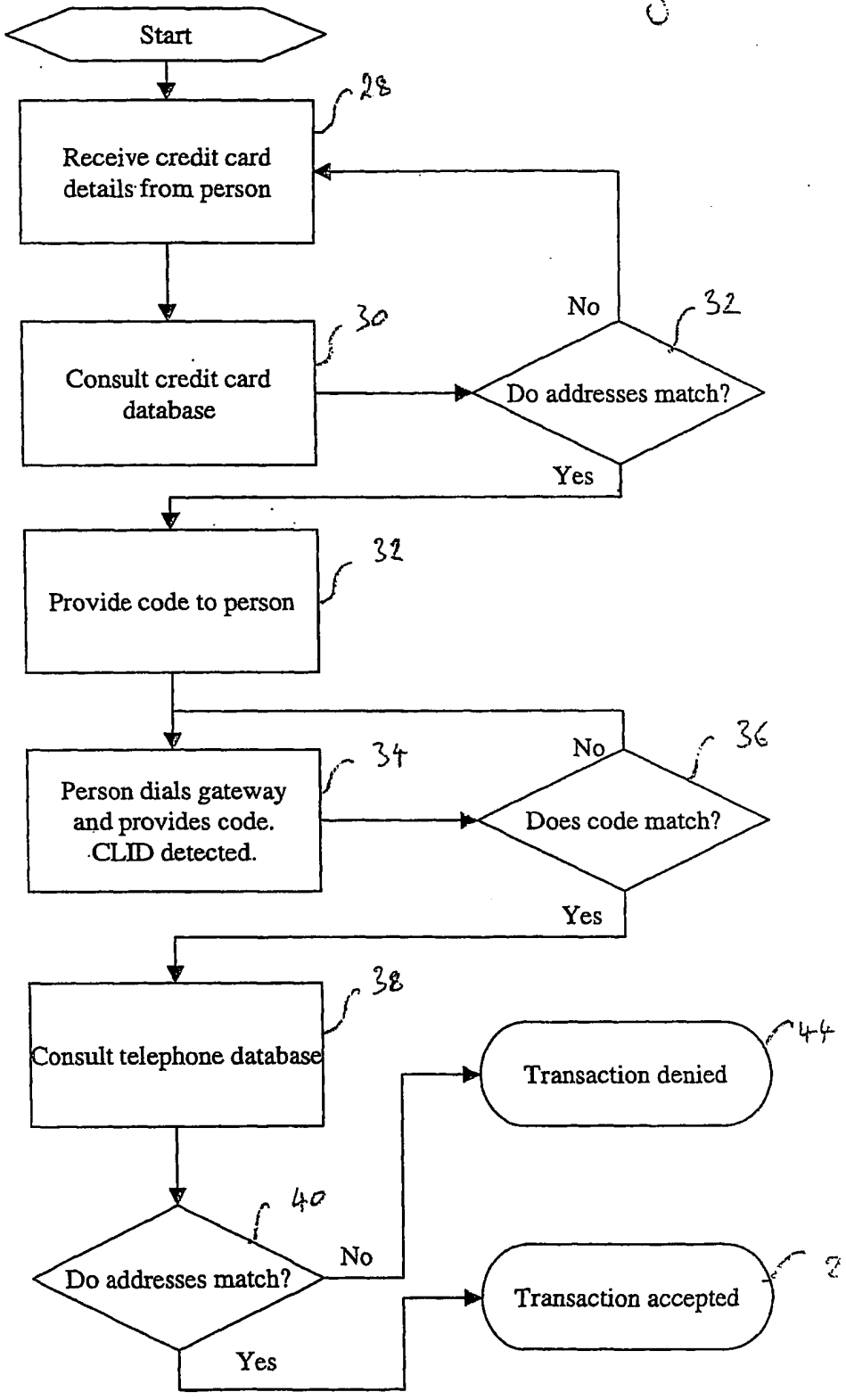


Fig 1

Fig 2


Start
28
Receive credit card details from person
30
Consult credit card database
No
32
Do addresses match?
Yes
32
Provide code to person
34
Person dials gateway and provides code. CLID detected.
No
36
Does code match?
Yes
38
Consult telephone database
44
Transaction denied
40
Do addresses match?
No
Transaction accepted
Yes

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/01269

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl. [7]: G07F 19/00, G06F 157:00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPAT: G06F, G07F, G06K + *KEYWORDS*: - CREDIT CARD, FRAUD, PREVENT, REDUCE, PHONE, AUTHENTICATE, VERIFY; POSTAL, STREET, HOME, PRIVATE ADDRESS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5311594 A (PENZIAS) 10 May 1994 Entire document, see abstract, and col. 5 lines 27-56	1-23
Y	US 5193114 A (MOSELEY) 9 March 1993 Entire document, see abstract, and col. 6	1-23
Y	US 5802156 A (FELGER) 1 September 1998 Entire document, see abstract, and col. 4-6	1-23

[X] Further documents are listed in the continuation of Box C [X] See patent family annex

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
28 October 2002	0 2 NOV 2002
Name and mailing address of the ISA/AU	Authorized officer
AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	**CHARLES BERKO** Telephone No : (02) 6283 2169

INTERNATIONAL SEARCH REPORT

International application No.
PCT/AU02/01269

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5991372 A (DAVENPORT D' INGIANNI et al.) 23 November 1999 Entire document	1-23
Y	WO 01/09854 A (CLAY-SMITH) 8 February 2001 Entire document	1-23
Y	WO 91/06915 A (GOODMAN) 16 May 1991 Entire document	1-23
Y	WO 01/52205 A (SEAGLADE DEVELOPMENTS LIMITED) 19 July 2001 Entire document	1-23

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/AU02/01269

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
US	5311594	CA	2114562	EP	618552	JP	7046323
US	5193114	NONE					
US	5802156	US	5933480	US	5960069	US	6282276
		US	5894510				
US	5991372	NONE					
WO	200109854	AU	200063096	EP	1200944		
WO	9106915	US	5146403	AU	70344/91	CA	2066577
		EP	498859	AU	68732/91	WO	9106906
		US	5132915	AU	69548/91	EP	500805
		WO	9106913				
WO	200152205	AU	200127007				

END OF ANNEX